A SECURE STORAGE UTILITY

Abstract of the Disclosure

A system and method implementing advanced cryptographic techniques to protect both the confidentiality and integrity of data sent to and received from a storage system or storage utility. Particularly, the system and method provides for the privacy and integrity of stored data. The integrity protection scheme employed defends against modification of data as well as "replay" and "relocation" of data since cryptographic integrity values are not only a function of the plaintext data and a cryptographic key, but also a function of the "address" of the disk block and a "whitening" value that defends against "replay attacks". The integrity scheme protects the integrity of an entire virtual disk while allowing incremental, random access updates to the blocks on the virtual disk.